

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
16.01.2002 Bulletin 2002/03

(51) Int Cl.⁷: **G11C 16/22**, G11C 8/00,
G11C 7/24

(21) Application number: **01305122.2**

(22) Date of filing: 13.06.2001

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(72) Inventors:

- Takata, Hidekazu
Nara-shi, Nara (JP)
- Sumitani, Ken
Tenri-shi, Nara (JP)

(30) Priority: 15.06.2000 JP 2000180627

(74) Representative: **Brown, Kenneth Richard et al**
R.G.C. Jenkins & Co. 26 Caxton Street
London SW1H 0RJ (GB)

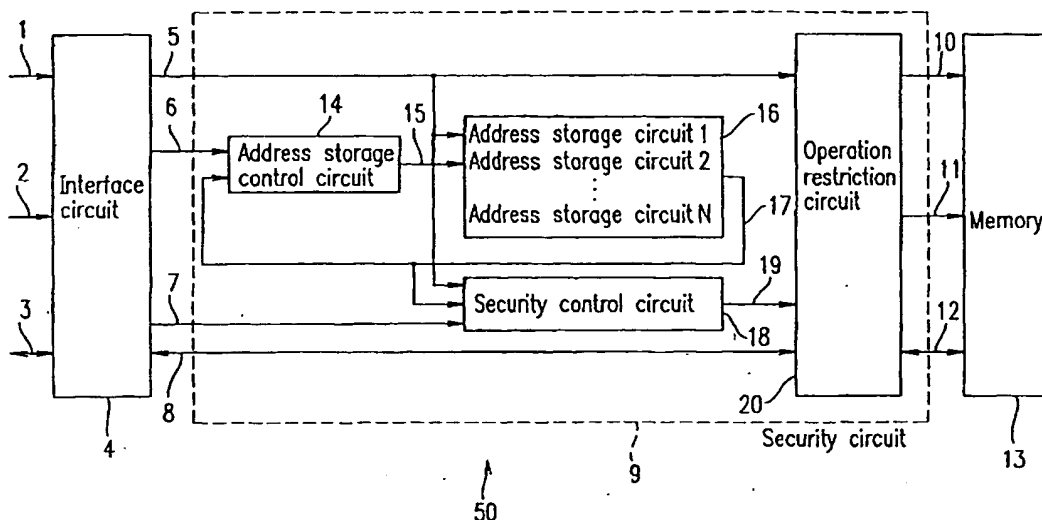
**(71) Applicant: Sharp Kabushiki Kaisha
Osaka-shi, Osaka 545-8522 (JP)**

(54) Semiconductor device and control device for use therewith

(57) A semiconductor device includes: a memory having a memory space for recording data, the memory space including addresses; at least one first storage section for storing at least a portion of an address at which access to the memory space is requested and/or data which is requested to be written to the memory

space; and an operation restriction circuit for at least partially restricting operations to be performed on the memory. The operation restriction circuit controls restriction on the operations to be performed on the memory based on at least a portion of the data and/or the address stored in the at least one first storage section.

FIG. 1



Description

BACKGROUND OF THE INVENTION

1. FIELD OF THE INVENTION:

[0001] The present invention relates to a semiconductor device having a memory space composed of rewritable semiconductor memory cells, and a control device for use therewith. In particular, the present invention relates to a semiconductor device having a security function for protecting from unauthorized access any content which is stored in the memory space, and a control device for use therewith.

2. DESCRIPTION OF THE RELATED ART:

[0002] A semiconductor device such as a semiconductor memory device has a memory space composed of rewritable semiconductor memory cells which are represented by respective addresses. A semiconductor memory device may store information (such as copyright-protected subject matter or privacy information of individuals) which should not be subjected to unauthorized reading by a third party, or information which should not be subjected to unauthorized overwriting (as in the case of IC card applications). There have been proposed some semiconductor devices having a memory space, and control devices for use therewith, which have a security function for protecting the stored contents (data) from such unauthorized access.

[0003] Hereinafter, a conventional semiconductor device having a security function will be described with reference to Figures 5 to 7.

[0004] Figure 5 is a schematic block diagram illustrating a minimum structure for realizing a security function. A semiconductor device 600 shown in Figure 5 includes a memory accessing means 604, a memory 613 having a memory space (semiconductor memory cells) for storing data, and a security means 609 inserted therebetween. With the security means 609, it is possible to restrict some or all of the operations which are externally requested.

[0005] The memory accessing means 604 externally receives an address signal 601, a control signal 602, and a data signal 603, and outputs an address signal 605 which designates one or several of the storage units (semiconductor memory cells) in the memory space of the memory 613 to which access is to be made; a control signal 607 which designates the type and/or content of access to be performed to the memory 613; and a data signal 608 which is used for inputting or outputting of data in accordance with the designated content in the memory 613.

[0006] The security means 609 is capable of restricting some or all of the operations which are represented by a signal which is output from the memory accessing means 604 to the memory 613. For example, the secu-

urity means 609 is capable of restricting the reading of any content which is stored in the memory 613, restricting the overwriting of any content which is stored in the memory 613, or both.

[0007] A given operation which is instructed by the memory accessing means 604 to be performed on the memory 613 is represented by the address signal 605, the control signal 607, and the data signal 608 which are output to the security means 609. In the case where the content of the operation which is instructed by the memory accessing means 604 to be performed on the memory 613 is permitted, the security means 609 outputs an address signal 610, a control signal 611, and a data signal 612 to the memory 613 to perform an operation as instructed by the memory accessing means 604. On the other hand, in the case where the content of the operation which is instructed by the memory accessing means 604 to be performed on the memory 613 is not permitted, the security means 609 applies a conversion process to at least one of the address signal 610, the control signal 611, and the data signal 612. If the externally instructed operation involves outputting of the data which is stored in the memory 613, the security means 609 applies a conversion process to the data signal 608 which is output from the security means 609 to the memory accessing means 604. Thus, the operations to the memory 613 are restricted so that any operations which are not permitted will not occur, thereby realizing a security function for the memory 613.

[0008] All of the component elements of the semiconductor device 600 shown in Figure 5 may be provided on one device. Alternatively, the component elements may be distributed over a number of devices so that a security function will be realized when the devices are used in combination. For example, in the case where the security function is to be realized on a single device, an interface circuit for interfacing with the exterior of the device may be utilized as the memory accessing means 604, while a circuit for restricting some or all of the operations which require access to the memory space may be inserted (as the security means 609) between the memory 613 as a circuit having a memory space and the memory accessing means 604.

[0009] Alternatively, in the case where the security function is to be realized on a number of devices collectively, e.g., when the memory accessing means 604, the security means 609, and the memory 613 are all provided on discrete devices, a circuit for restricting some or all of the operations which require access to the memory space may be inserted (as the security means 609) between a memory controller functioning as the memory accessing means 604 and the memory 613 having a memory space.

[0010] Hereinafter, a semiconductor device which is capable of outputting dummy data when a read access to the memory is made will be specifically described, by an illustration of a structure in which read operations to a memory are restricted until deactivation of a security

function.

[0011] Figure 6 is a schematic block diagram illustrating a conventional semiconductor device 450 which realizes the above-described security function. The semiconductor device 450 includes an interface circuit 404, a security circuit 409, and a memory 413 having a memory space composed of semiconductor memory cells. The security circuit 409 includes a password storage circuit 414 for storing a password, a comparison circuit 416, and an operation restriction circuit 418 for restricting operations to be performed on the memory 413.

[0012] In accordance with the semiconductor device 450, restriction on read operations is established (i.e., a security function is set) at the time when the semiconductor device 450 is turned ON. The security function can only be deactivated if a password (security control signal) 407 which is externally input via the interface circuit 404 matches a fixed password which is stored in the password storage circuit 414 in the security circuit 409; after which read operations can be performed normally.

[0013] In the case of making an external access to the stored content (data) which is stored in a given address in the memory 413 of the semiconductor device 450, an address signal 401, a control signal 402, and a data signal 403 are input to the interface circuit 404. The interface circuit 404 outputs an internal address signal 405 and an internal control signal 406, and if necessary an internal data signal 408, to the memory 413. In the case where the security function of the memory 413 is deactivated, the operation restriction circuit 418 outputs an address signal 410, a control signal 411, and a data signal 412 to the memory 413 in accordance with the address signal 401, the control signal 402, and the data signal 403, which are externally supplied (or more directly, in accordance with the internal address signal 405, the internal control signal 406, and the internal data signal 406). As a result, a normal operation is performed.

[0014] The semiconductor device 450 is constructed in such a manner that the security function of the memory 413 is set in an initial state which follows after the semiconductor device 450 is turned ON. As a result of the restriction on some or all of the operations to the memory 413 enforced by the security circuit 409, the semiconductor device 450 either refrains from operating at all or performs an operation which is different from an instructed operation. In applications which are arranged so as to output dummy data (instead of normal data) when a read access to the memory 413 is made, once the security function is set, only the dummy data will be output in response to any read access made to the memory 413, thereby preventing any unauthorized reading.

[0015] The following methods have been proposed as methods for realizing the aforementioned function of preventing unauthorized read. For example, a method described in Japanese Laid-Open Publication No. 59-152599 ensures that, while the security function is

activated, the address signal 410 is not output from the security circuit 409 to the memory 413 unless certain conditions are satisfied. According to a method described in Japanese Laid-Open Publication No. 6-250939, the security circuit 409 encrypts the data signal 412 received by the memory 413 and outputs the encrypted version of the data signal 412 to the interface circuit 404 as the data signal 408. According to yet another method, it is ensured that, while the security function is activated, the security circuit 409 does not output the control signal 411 to the memory 413 for instructing a read operation to be commenced unless certain conditions are satisfied.

[0016] In order to deactivate the read restriction for the memory 413, a password (security control signal) 407 for deactivating the operation restriction is externally input. The externally input password 407 is compared by the comparison circuit 416 against a password signal 415 representing a password which is stored in the password storage circuit 414. If both passwords match, the comparison circuit 416 issues an operation restriction deactivating signal (password match signal) 417 to the operation restriction circuit 418. Upon receiving the operation restriction deactivating signal 417, the operation restriction circuit 418 permits any subsequent read operations to be performed to the memory. Thereafter, read operations will be normally performed upon request of a read.

[0017] Based on the above structure, the stored content in the memory cannot be properly read by a person who does not know the password and a method for inputting the password. Thus, unauthorized reading by a third party can be prevented if the password and the method for inputting the password are not made public.

[0018] Figure 7 is a schematic block diagram illustrating a system 500 which realizes a security function for a semiconductor device by employing a different structure from that illustrated in Figure 6. The system 500 includes control device 501 (e.g., CPU) which requests access to the memory, a semiconductor device 550 having a security function, and a security control device 506. In the system 500, the control device 501 outputs an address signal 502, a control signal 503, and a data signal 505 to the semiconductor device 550 to perform an operation on the semiconductor device 550. However, the control device 501 cannot take full control of the semiconductor device 550 unless the security function of the semiconductor device 550 is deactivated.

[0019] The security control device 506 is "challenged" to deactivate the security function of the semiconductor device 550 as follows. The security function of the semiconductor device 550 is deactivated only when the semiconductor device 550 recognizes from the content of a security communication signal 504 that the security control device 506 is a device which is predetermined to be granted access thereto. If the transmitter/recipient of the security communication signal 504 is not recognized as the predetermined device, the security function

is not deactivated, and some or all of the operations to be performed on the semiconductor device 550 remain restricted.

[0020] During an initial state after the system 500 is turned ON, the security function of the system 500 is activated, so that the contents stored in the semiconductor device 550 cannot be properly read by an external device. The semiconductor device 550 "challenges" the security control device 506, i.e., transmits to the security control device 506 a signal (security communication signal) 504 for recognizing what device is being coupled to the semiconductor device 550, and the security control device 506 returns a signal which the security control device 506 generates based on the signal 504. The semiconductor device 550 determines whether or not the returned signal 504 matches an expected value. If the returned signal 504 matches the expected value, it is determined that the proper (or authorized) security control device 506 is coupled to the semiconductor device 550 as an external device, and accordingly deactivates the security function of the semiconductor device 550. The transmission/reception of the signal 504 may be repeated multiple times to gain enhanced security.

[0021] Unlike the security function of the semiconductor device 450 shown in Figure 6, the system 500 provides a security function which may be enforced in such a manner that the "right" communication to occur between the semiconductor device 550 and the security control device 506 is directed to a different content each time such a communication is made. Therefore, the security function provided by the system 500 is difficult to break via simple signal analysis.

[0022] Thus, the semiconductor device 550 can provide a very secure security function because it permits a proper read operation to occur only when the security control device 506 coupled thereto is recognized as a predetermined device.

[0023] Instead of the above-described example where unauthorized reading is prevented, a security function can also be realized to restrict other types of operations as well. For example, in order to prevent unauthorized overwriting of the content stored in a memory, the same conditions as those described above for establishing or deactivating restriction on read operations can be applied for establishing or deactivating restriction on overwrite operations.

[0024] However, the above-described conventional method for realizing a security function has the following problems.

[0025] In the semiconductor device 450 shown in Figure 6, since a fixed protocol is always used for deactivating the security function, a third party may relatively easily discover a security deactivating method by analyzing the input signals, e.g., the password (security control signal) 407.

[0026] On the other hand, the system 500 shown in Figure 7, the content of the output (i.e., the security communication signal 504) from the security device 506

which is expected by the semiconductor device 550 can be varied, whereby a more secure security function can be realized. However, this structure has cost and/or size-related disadvantages associated with the security control device 506, which needs to be provided externally to the semiconductor device 550.

SUMMARY OF THE INVENTION

[0027] In one aspect of the present invention, there is provided a semiconductor device including: a memory having a memory space for recording data, the memory space including addresses; at least one first storage section for storing at least a portion of an address at which access to the memory space is requested and/or data which is requested to be written to the memory space; and an operation restriction circuit for at least partially restricting operations to be performed on the memory, wherein the operation restriction circuit controls restriction on the operations to be performed on the memory based on at least a portion of the data and/or the address stored in the at least one first storage section.

[0028] In accordance with the above structure, it is possible to control restriction on operations to be performed on the memory by utilizing at least a portion of data requested to be written to the memory space and/or an address at which the data is requested to be written. Some or all of the operations requiring any access to the memory space can be restricted until the operation restriction circuit deactivates restriction on operations to be performed on the memory, for example. Thus, it is difficult for a third party to decipher the method for deactivating the security function. Since it is not necessary to provide any special devices external to the semiconductor device for realizing the security function, there is no substantial penalty associated with the product size and/or cost.

[0029] In one embodiment of the invention, the access is a write operation.

[0030] In another embodiment of the invention, the at least one first storage section comprises a plurality of storage subsections.

[0031] In accordance with the above structure, (a portion of) a plurality of data requested to be written to the memory space and/or a plurality of addresses at which the data is requested to be written can be stored. Thus, it becomes even more difficult for a third party to decipher the method for deactivating the security function, whereby a semiconductor device can be realized which cannot be easily subjected to unauthorized utilization.

[0032] In another embodiment of the invention, if at least one of the at least one first storage section does not contain the address or data stored therein, the operation restriction circuit maintains restriction on the operations to be performed on the memory.

[0033] In accordance with the above structure, security can be provided in a state (e.g., an initial state)

where not all of the storage subsections contain (a portion of) data and/or an address.

[0034] In still another embodiment of the invention, the at least one first storage section includes an address storage section for storing the address, and a data storage section for storing the data; the semiconductor device includes a comparison circuit for performing a comparison of data in the memory space as designated by the address stored in the address storage section against the data stored in the data storage section; and the operation restriction circuit maintains restriction on the operations to be performed on the memory if a result of the comparison by the comparison circuit does not match.

[0035] In accordance with the above structure, a higher level of security can be realized because it is possible to confirm at the time of a read operation that the stored data has not been altered.

[0036] In still another embodiment of the invention, the semiconductor device further comprises: a second storage section for storing a reference address; and a comparison circuit for performing a comparison of the address stored in the first storage section against the reference address stored in the second storage section, wherein the operation restriction circuit deactivates restriction on the operations to be performed on the memory if a result of the comparison by the comparison circuit matches.

[0037] In accordance with the above structure, a higher level of security can be realized by comparing the addresses stored in the first storage section against the reference addresses stored in the second storage section.

[0038] In still another embodiment of the invention, the memory includes a storage unit for containing data which is to be concurrently rewritten; and the first storage section is included in the storage unit.

[0039] In accordance with the above structure, it becomes possible to vary security conditions by concurrently rewriting the contents stored in at least a portion of the memory space of the memory and the first storage section, whereby a higher level of security can be provided. Note that the second storage section should not be formed within the memory rewriting unit because if the second storage section were formed within the memory rewriting unit, the content stored in the second storage section would be lost when the rewriting unit is overwritten, thereby allowing a user an opportunity to freely set the content after the overwriting.

[0040] In another aspect of the present invention, there is provided a control device for controlling a memory having a memory space for recording data, the memory space including addresses, the control device comprising: at least one first storage section for storing at least a portion of an address at which access to the memory space is requested and/or data which is requested to be written to the memory space; and an operation restriction circuit for at least partially restricting

operations to be performed on the memory, wherein the operation restriction circuit controls restriction on the operations to be performed on the memory based on at least a portion of the data and/or the address stored in the at least one first storage section.

[0041] In accordance with the above structure, it is possible to control restriction on operations to be performed on the memory by utilizing at least a portion of data requested to be written to the memory space and/or an address at which the data is requested to be written. Some or all of the operations requiring any access to the memory space can be restricted until the operation restriction circuit deactivates restriction on operations to be performed on the memory, for example. Thus, it is difficult for a third party to decipher the method for deactivating the security function. By embedding the security function in any device (e.g., a memory controller) on a given system other than the memory, the penalty associated with the product size and/or cost can be reduced.

[0042] In one embodiment of the invention, the access is a write operation.

[0043] In another embodiment of the invention, the at least one first storage section comprises a plurality of storage subsections.

[0044] In accordance with the above structure, it becomes even more difficult for a third party to decipher the method for deactivating the security function, whereby a control device can be realized which cannot be easily subjected to unauthorized utilization.

[0045] In another embodiment of the invention, if at least one of the at least one first storage section does not contain the address or data stored therein, the operation restriction circuit maintains restriction on the operations to be performed on the memory.

[0046] In accordance with the above structure, security can be provided in a state (e.g., an initial state) where not all of the storage subsections contain (a portion of) data and/or an address.

[0047] In still another embodiment of the invention, the at least one first storage section includes an address storage section for storing the address, and a data storage section for storing the data; the semiconductor device includes a comparison circuit for performing a comparison of data in the memory space as designated by the address stored in the address storage section against the data stored in the data storage section; and the operation restriction circuit maintains restriction on the operations to be performed on the memory if a result of the comparison by the comparison circuit does not match.

[0048] In accordance with the above structure, a higher level of security can be realized because it is possible to confirm at the time of a read operation that the stored data has not been altered.

[0049] In still another embodiment of the invention, the control device further comprises: a second storage section for storing a reference address; and a compar-

ison circuit for performing a comparison of the address stored in the first storage section against the reference address stored in the second storage section, wherein the operation restriction circuit deactivates restriction on the operations to be performed on the memory if a result of the comparison by the comparison circuit matches.

[0050] In accordance with the above structure, a higher level of security can be realized by comparing the addresses stored in the first storage section against the reference addresses stored in the second storage section.

[0051] In still another embodiment of the invention, the memory includes a storage unit for containing data which is to be concurrently rewritten; and the first storage section is included in the storage unit.

[0052] In accordance with the above structure, it becomes possible to vary security conditions by concurrently rewriting the contents stored in at least a portion of the memory space of the memory and the first storage section, whereby a higher level of security can be provided. Note that the second storage section should not be formed within the memory rewriting unit because if the second storage section were formed within the memory rewriting unit, the content stored in the second storage section would be lost when the rewriting unit is overwritten, thereby allowing a user an opportunity to freely set the content after the overwriting.

[0053] Thus, the invention described herein makes possible the advantages of: (1) providing a semiconductor device having a security function for preventing unauthorized read or overwrite which can be deactivated by a method which is difficult for any unauthorized third party to analyze and decipher, such that the security function can be realized without the need to require a special external device; and (2) providing a control device for such a semiconductor device.

[0054] These and other advantages of the present invention will become apparent to those skilled in the art upon reading and understanding the following detailed description with reference to the accompanying figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[0055] Figure 1 is a schematic block diagram illustrating a semiconductor device incorporating a control device for a memory according to Example 1 of the present invention.

[0056] Figure 2 is a schematic block diagram illustrating a semiconductor device incorporating a control device for a memory according to Example 2 of the present invention.

[0057] Figure 3 is a schematic block diagram illustrating a semiconductor device incorporating a control device for a memory according to Example 3 of the present invention.

[0058] Figure 4 is a schematic block diagram illustrating a semiconductor device incorporating a control device for a memory according to Example 4 of the present

invention.

[0059] Figure 5 is a schematic block diagram illustrating a security function in a semiconductor device.

[0060] Figure 6 is a schematic block diagram illustrating a conventional semiconductor device.

[0061] Figure 7 is a schematic block diagram illustrating a conventional semiconductor memory device.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0062] Hereinafter, the present invention will be described by way of illustrative examples, with reference to the accompanying figures.

(Example 1)

[0063] Figure 1 is a schematic block diagram illustrating a semiconductor device 50 having a memory space composed of rewritable semiconductor memory cells according to Example 1 of the present invention. The semiconductor device 50 includes an interface circuit 4, a security circuit 9, and a memory 13 (defining a memory space) composed essentially of rewritable semiconductor memory cells. In general, a "memory space" includes a plurality of addresses, where data can be recorded corresponding to each address.

[0064] The security circuit 9 includes: an address storage control circuit 14; an address storage circuit section 16 capable of storing N addresses; a security control circuit 18; and an operation restriction circuit 20 for restricting the operations to be performed on the memory 13. The security circuit 9 functions as a control circuit for the memory 13. It is assumed that the address storage circuit section 16 includes N address storage circuits 1 to N (where N is a natural number), such that each of the address storage circuits 1 to N stores one address. Each of the address storage circuits 1 to N functions as a storage subsection.

[0065] The memory 13 may include volatile semiconductor memory cells (as in static RAMs) or non-volatile semiconductor memory cells (as in EEPROMs).

[0066] All of the component elements of the semiconductor device 50 may be provided on one device to realize a security function for the memory 13. However, it is not necessary to provide all of the aforementioned component elements on a single device. For example, the security function may be realized on a number of devices collectively, e.g., by employing a separate security device, which includes the interface circuit 4 and the security circuit 9, to control the memory 13.

[0067] Hereinafter, a security protocol of the semiconductor device 50 according to the present invention, i.e., a method for restricting operations which require access to the memory space composed of rewritable semiconductor memory cells, will be described. The following description will be directed to an instance of "unauthorized read prevention function" where, when a por-

tion of data is to be read from a partial region of the memory 13, dummy data is output in the place of the actual data, thereby restricting the read operations to be performed to the data stored in the memory.

[0068] The semiconductor device 50 receives an address signal 1, a control signal 2, and a data signal 3, which are externally input for the purpose of reading data stored at a given address of the memory 13.

[0069] Upon analyzing the address signal 1, the control signal 2, and the data signal 3, the interface circuit 4 recognizes that a read operation has been externally issued for the semiconductor device 50. Accordingly, the interface circuit 4 outputs an internal address signal 5 and an internal control signal 6 to instruct that data stored at an address in the memory space which is designated by the internal address signal 5 be transmitted via an internal data signal 8. The interface circuit 4 includes a circuit for analyzing externally-input signals, and a state machine for controlling the operation of controlling the stored content in the semiconductor device 50, a circuit for controlling an output signal in accordance with external requests, and the like. The exact structure of the interface circuit 4 may vary depending on the specification of the semiconductor device 50.

[0070] The security circuit 9 outputs the address signal 10 and the control signal 11 to the memory 13, and reads the content which is stored in the memory 13 via the data signal 12. In the initial state, the security control circuit 18 is reset, and an internal control signal 19 is issued to indicate to the operation restriction circuit 20 that the security function has not been deactivated. The operation restriction circuit 20 examines the received internal address signal 5, and upon determining that the address represented by the internal address signal is a predetermined address, exchanges the data which is read from the memory 13 (i.e., the data signal 12) with dummy data, and outputs an internal data signal 8 representing the dummy data to the interface circuit 4.

[0071] The interface circuit 4 receives the dummy data via the internal data signal 8, and outputs the dummy data to an external device via the data signal 3. Thus, it is made impossible to perform a proper read operation from that particular address. As a result, the unauthorized reading or utilization of the content stored in the semiconductor device 50 can be prevented.

[0072] Instead of exchanging the data represented by the data signal 12 with dummy data, the operation restriction circuit 20 can utilize various methods as a means for restricting the reading from the memory 13, without limitation. For example, an address represented by the address signal 5 may be exchanged with a dummy address which is output to the memory 13 as the address signal 10. Alternatively, the control signal 11, which is used to instruct reading from the memory 13, may be prevented from being output.

[0073] As the operation restriction circuit 20, any circuit structure that restricts an operation (which is not limited to a read operation) which requires access to the

memory space may be employed. For example, when an overwriting of the data stored in the memory 13 is externally instructed, the address represented by the address signal 5 may be exchanged with a dummy address to be output as the address signal 10. Alternatively, the data represented by the data signal 8 may be exchanged with dummy data to be output to the memory 13 as the data signal 12. Thus, any externally-instructed operation which requires access to the memory space of the memory 13 can be prevented from occurring properly. As a result, the unauthorized use of the semiconductor device can be prevented.

[0074] Next, the security deactivation protocol of the semiconductor device 50 will be described.

[0075] An address signal 1, a control signal 2, and a data signal 3 are externally input to the semiconductor device 50. When an overwriting of the data at a given address of the memory 13 is requested (assuming that not all of the address storage circuits 1 to N in the address storage circuit section 16 contain addresses stored therein), the address storage control circuit 14 issues an address storage control signal 15, whereby an address for which an overwriting has been requested is stored in the address storage circuit section 16. In the address storage circuit section 16, addresses are sequentially stored in the address storage circuits 1 to N, beginning from the address storage circuit 1. The address storage control circuit 14 determines whether or not addresses are stored in all of the address storage circuits 1 to N based on an address signal 17 which is output from the address storage circuit section 16. If addresses are stored in all of the address storage circuits 1 to N, the address storage control circuit 14 does not issue the address storage control signal 15 so that no more addresses will be stored.

[0076] If at least one of the address storage circuits 1 to N in the address storage circuit section 16 does not contain an address stored therein, the security function cannot be deactivated. If all of the address storage circuits 1 to N contain addresses stored therein, security deactivation is performed by using the stored addresses. As the information stored in the address storage circuits, only some of the bits representing each address may be stored, rather than all of the bits representing each address, because the order of overwriting is significant, as opposed to the address value itself.

[0077] Alternatively, the address storage control circuit 14 may be a circuit which, based on the address signal 17, detects one or more of the address storage circuits 1 to N which do not contain any addresses stored therein, and outputs the address storage control signal 15 to instruct, when the internal control signal 6 is issued to request an address to be stored, that the address signal 5 be stored in the circuit(s) (1 to N) in which address(es) are not stored.

[0078] Each of the address storage circuits 1 to N in the address storage circuit section 16 may be a circuit which includes as many register circuits as the number

of bits representing an address to be stored, and a register circuit for storing a bit indicating that an address is stored in the circuit. In this case, one of the address storage circuits 1 to N which has been instructed to store an address represented by the address signal 5 based on the address storage control signal 15 stores the address represented by the address signal 5 in the register circuits within the address storage circuit, and further sets a bit indicating that an address is stored in the address storage circuit.

[0079] As a method for deactivating the security function, for example, a method may be employed in which the security control circuit 18 uses an address stored in the address storage circuit section 16 as a password, requiring a security control signal 7 to be input. The security control signal 7 is generated in the interface circuit 4 based on an externally input signal.

[0080] Alternatively, as described in Japanese Application No. 2000-121844, a method may be employed in which the addresses of a memory are read in a certain sequence, and in which the security function is deactivated only when the values and order of the addresses match those stored in the address storage circuit section 16. Furthermore, as described in Japanese Laid-Open Publication No. 3-204053 or Japanese Laid-Open Publication No. 1-1.73244, a technique of utilizing for security control the information as to whether the order of addresses in a read operation is proper or not may be employed. Note that the present invention employs a different method from the method for storing addresses in the address storing regions according to Japanese Application No. 2000-121844, *supra*. According to Japanese Application No. 2000-121844, *supra*, it is necessary to externally designate storage of fixed data in the address storing regions, so that it is necessary to make public the means for storing security information. In contrast, according to the present invention, such a storage operation can itself be concealed within the usual operations of the semiconductor device. As a result, a security function can be realized without risking any public disclosure.

[0081] The aforementioned security deactivation is realized by the security control circuit 18. The security control circuit 18 outputs a security control signal 19 to instruct the deactivation of the security function to the operation restriction circuit 20. Once receiving the security control signal 19 which instructs the deactivation of the security function, the operation restriction circuit 20 no longer applies restriction on any read operations which are requested to be performed on the memory 13. As a result, read operations can take place properly.

[0082] As the security control circuit 18, a circuit which examines an order in which a number of addresses were accessed, e.g., as described in Japanese Application No. 2000-121844, *supra*, may be employed.

[0083] Although the present example illustrates a case in which unauthorized reading is prevented, the present invention is not limited thereto. It will be appre-

ciated that the present invention is also applicable to restriction of any other types of access to the memory space, e.g., overwriting. For example, in the case where the present invention is used for restricting overwrite operations, a method can be employed in which the operation restriction circuit 20 outputs as an address signal 10 to the memory 13 a dummy address which is not identical to an address which has been requested to be overwritten (as represented by the address signal 5). Alternatively, a method may be employed in which a control signal 11 for instructing overwrite is prevented from being output to the memory 13 unless the security function is deactivated. Alternatively, a method may be employed in which data (i.e., dummy data) which is not identical to the data which has been requested to be overwritten (as represented by the internal data signal 8) is output as a data signal 12 to the memory 13. Thus, it is possible to restrict overwrite operation in a manner similar to restricting read operations as discussed above.

(Example 2)

[0084] Figure 2 is a schematic block diagram illustrating a semiconductor device 150 according to Example 2 of the present invention. The semiconductor device 150 includes an interface circuit 104, a security circuit 109, and a memory 113 (defining a memory space) composed essentially of rewritable semiconductor memory cells.

[0085] The security circuit 109 includes: address/data storage control circuit 114; an address storage circuit section 116 capable of storing N addresses (where N is a natural number); a data storage circuit section 121 capable of storing M units of data (where M is a natural number); an address comparison circuit 118; a data comparison circuit 123; a security control circuit 125; and an operation restriction circuit 127 for restricting the operations to be performed on the memory 113. The security circuit 109 functions as a control circuit for the memory 113.

[0086] In the present example, it is assumed that the address storage circuit section 116 includes N address storage circuits 1 to N, such that each of the address storage circuits 1 to N stores one address. It is also assumed that the data storage circuit section 121 includes M data storage circuits 1 to M, such that each of data storage circuits 1 to M stores one unit data. Each of the address storage circuits 1 to N and each of data storage circuits 1 to M functions as a storage subsection.

[0087] All of the component elements of the semiconductor device 150 may be provided on one device to realize a security function for the memory 113. However, it is not imperative that the semiconductor device 150 is realized as a single device. For example, the security function may be realized on a number of devices collectively, e.g., by employing a separate security device, which includes the interface circuit 104 and the security

circuit 109, to control the memory 113.

[0088] Although the following description is directed to a case where the number N of addresses which can be stored in the address storage circuit section 116 and the number M of data which can be stored in the data storage circuit section 121 are equal ($N=M$), it is not necessary that M and N be equal. In the present example, the memory 113, the interface circuit 104, and the operation restriction circuit 127 may be implemented by using similar means to the memory 13, the interface circuit 4, and the operation restriction circuit 20 according to Example 1.

[0089] Hereinafter, a security protocol of the semiconductor device 150 according to the present invention will be described. The following description will be directed to an instance of "unauthorized read prevention function" where an output resulting from a read operation to a partial region of the memory 113 is exchanged with dummy data, thereby restricting the read operations to be performed to the data stored in the memory.

[0090] The semiconductor device 150 receives an address signal 101, a control signal 102, and if necessary a data signal 103, which are externally input for the purpose of reading data stored in the memory 113. During an initial state which follows after the semiconductor device 150 is turned ON, the reading of at least a partial address region of the memory 113 is restricted. Unless the security function is deactivated, the operation restriction circuit 127 prevents a read operation from properly occurring, as may be realized by: outputting a signal which is obtained by subjecting a data signal 112 having been read from the memory 113 to a predetermined mathematical operation as an internal data signal 108 to the interface circuit 104; withholding a control signal 111 from being issued to the memory 113; or outputting an address which is obtained by converting an address represented by an internal address signal 105 as an address signal 110.

[0091] Next, the security deactivation protocol of the semiconductor device 150 will be described.

[0092] In the case where a request for overwriting the data stored in a given address is externally made to the semiconductor device 150 by using the address signal 101, the control signal 102, and the data signal 103, then the address/data storage control circuit 114 stores the address for which overwrite has been requested in any address storage circuit within the address storage circuit section 116 where addresses are not stored yet. In doing so, it is ensured that addresses are sequentially stored in the address storage circuits 1 to N, beginning from the address storage circuit 1. At the same time, any data which is sought to be written in the memory 113 is sequentially stored in the data storage circuits 1 to M (assuming $N=M$), beginning from the data storage circuit 1. The address/data storage control circuit 114 no longer stores such addresses or data if all of the address storage circuits 1 to N or if all of the data storage circuits 1 to M (assuming $N=M$) already contain addresses and

data stored therein.

[0093] According to the present example, storage of addresses is controlled based on an internal control signal (address storage control signal) 106 which is output from the interface circuit 104, and storage of data is controlled based on an internal control signal (data storage control signal) 107 which is output from the interface circuit 104. If all of the address storage circuits 1 to N already contain addresses stored therein, or if all of the data storage circuits 1 to M contain data stored therein, the address/data storage control circuit 114 prevents further storage of addresses or data by not generating the address storage control signal 115 or the data storage control signal 120, respectively. When all of the address storage circuits 1 to N and all of the data storage circuits 1 to M contain addresses and data stored therein, the security function can be deactivated on the basis of the stored addresses and data. As the addresses or data to be stored in the address or data storage circuits, only portions of each address or data may be stored, rather than the entire address or data, because the order of overwriting is significant, as opposed to the address or data value itself. In the present example, the address/data storage control circuit 114 may be implemented by using similar means to the address storage control circuit 14 according to Example 1 of the present invention. The address storage circuit section 116 and the data storage circuit section 121 may be implemented by using similar means to the address storage circuit section 16 according to Example 1 of the present invention.

[0094] As a method for deactivating the security function, various methods can be employed. For example, as described in Japanese Application No. 2000-121844, supra, a method may be employed in which read operations are performed to the addresses of the memory 113 in a certain sequence, and in which the security function is deactivated only when the values and order of the addresses match those stored in the address storage circuit section 116. Alternatively, the following method may be employed. When read operations are performed, the address comparison circuit 118 compares an address (address signal 105) for which a read operation has been requested against an address (address signal 117) stored in the address storage circuit section 116, and outputs the result of the comparison as a matching detection signal 119 to the security control circuit 125. Moreover, the data comparison circuit 123 compares data which has been read via the data signal 112 against data which is stored in the data storage circuit section 121 (data signal 122), and outputs the result of the comparison as a matching detection signal 124 to the security control circuit 125. If it is detected by the security control circuit 125 that the addresses match but that the data do not match, it is determined that the stored content has been subjected to an unauthorized overwriting, and the security control circuit 125 outputs a security control signal 126 to control the operation restriction circuit 127, thereby ensuring that the security

function will not be deactivated. On the other hand, if it is detected by the security control circuit 125 that both the addresses and the data match, a signal instructing deactivation of the security function is output as a security control signal 126 to the operation restriction circuit 127. Once receiving the security control signal 126 which instructs the deactivation of the security function, the operation restriction circuit 127 no longer applies restriction on any read operations which are requested to be performed on the memory 113. As a result, read operations can take place properly.

[0095] As the security control circuit 125, a circuit which examines an order in which a number of addresses were accessed, e.g., as described in Japanese Application No. 2000-121844, supra, plus additional determination circuitry for determining not only matching of the address but also matching of the corresponding data, may be employed.

[0096] Although the present example illustrates a case in which unauthorized reading is prevented, the present invention is not limited thereto. As in Example 1, it will be appreciated that the present invention is also applicable to restricting any other types of access to the memory space, e.g., overwriting. For example, in the case where the present invention is used for restricting overwrite operations, a method can be employed in which the operation restriction circuit 127 cancels a requested overwrite operation, or performs an overwrite operation which is not identical to the requested overwrite operation. Thus, it is possible to restrict overwrite operations in a manner similar to restricting read operations as discussed above.

[0097] Although the above description illustrates a case where both the address stored in the address storage circuit section 116 and the data stored in the data storage circuit section 121 are utilized for realizing a security function, the effects of the present invention can also be obtained by utilizing only either one of the address stored in the address storage circuit section 116 or the data stored in the data storage circuit section 121, in a manner similar to using the address storage circuit section 16 according to Example 1.

(Example 3)

[0098] Figure 3 is a schematic block diagram illustrating a semiconductor device 250 according to Example 3 of the present invention. The semiconductor device 250 is configured in such a manner that the function of the address storage circuit section 16 in the semiconductor device 50 of Example 1 is embodied within a rewritable memory 225.

[0099] The semiconductor device 250 includes an interface circuit 204, a security circuit 209, and a memory 225 which includes at least one memory rewriting unit 214 having a memory space composed essentially of concurrently-rewritable semiconductor memory cells. The security circuit 209 includes an address storage

control circuit 215, a security control circuit 217, and an operation restriction circuit 219 for restricting the operations to be performed on the memory 225. The security circuit 209 functions as a control circuit for the memory 225.

[0100] The memory rewriting unit 214 includes address storing regions 1 to N which, as a whole, are capable of storing N addresses. Note that the address storing regions 1 to N included in the memory rewriting unit 214 correspond to the address storage circuits 1 to N in the address storage circuit section 16 of the semiconductor device 50 of Example 1.

[0101] The address storing regions 1 to N are preferably implemented by using address regions other than the address regions which are subject to regular requests for overwriting because the addresses stored in the address storing regions 1 to N, which are intended to be utilized as security information, may be destroyed through regular overwriting. For example, in the case where the present example is applied to a flash memory which is capable of block erasure, it would be preferable to provide extra row and/or column lines, in addition to those associated with addresses which are subjected to regular use, within each block to be concurrently erased; in this case, the memory cells which are coupled to the additional row lines and column lines can be used as the address storing regions 1 to N.

[0102] All of the component elements of the semiconductor device 250 may be provided on one device to realize a security function for the memory 225. However, it is not necessary to provide all of the aforementioned component elements on a single device. For example, the security function may be realized on a number of devices collectively, e.g., by employing a separate security device, which includes the interface circuit 204 and the security circuit 209, to control the memory 225 (including the memory rewriting unit 214).

[0103] As a security protocol for the semiconductor device 250, a method (e.g., the method described in Example 1) may be employed in which the operation restriction circuit 219 somehow modifies a data signal 212 representing the data read from the memory 225 before being output as an internal data signal 208.

[0104] As the method for concurrent rewriting, rewriting via a buffer, block erasure of a flash EEPROM, or other similar means may be used. Although the following description illustrates the case where the present invention is applied to a flash EEPROM which is capable of concurrent block erasure, the same technique can also be used for rewriting via a buffer. The following description is directed to the case where the data stored in the memory rewriting unit 214 cannot be erased unless restriction on erase operations is deactivated, thereby preventing unauthorized data overwriting.

[0105] An address signal 201, a control signal 202, and a data signal 203 are externally input to the semiconductor device 250 to request overwriting of data stored at a given address of the memory 225. Upon rec-

ognizing the request, the interface circuit 204 outputs an internal control signal 206 to the address storage control circuit 215. Determining that the address is within the memory rewriting unit 214, the address storage control circuit 215 outputs a signal 220 to the interface circuit 204. The interface circuit 204 reads the stored content in the address storing regions 1 to N, and stores the address for which overwrite has been requested in any address storing regions 1 to N where addresses are not stored yet. In addition to this operation, the data overwrite as externally requested is performed to the semiconductor device 250. In doing so, it is ensured that addresses are sequentially stored in the address storing regions 1 to N, beginning from the address storing region 1. The address storing regions 1 to N function as storage subsections.

[0106] If all of the address storing regions 1 to N already store addresses for which overwrite has been requested, the address storage control circuit 215 does not store any more addresses, and only performs regular data overwriting.

[0107] Upon determining that at least one of the address storing regions 1 to N does not contain an address stored therein, the address storage control circuit 215 outputs an address storage control signal 216 to the operation restriction circuit 219 so that the operation restriction circuit 219 prohibits erase operations from being performed on the memory rewriting unit 214. On the other hand, if all of the address storing regions 1 to N contain addresses stored therein, erase operations to the memory rewriting unit 214 are permitted on the basis of the stored addresses. As a method for prohibiting erase operations, for example, the operation restriction circuit 219 may withhold a control signal 211 from being issued to the memory 225. As the addresses to be stored in the address storing regions 1 to N, only portions of each address may be stored, rather than the entire address, because the order of overwriting is significant, as opposed to the address value itself.

[0108] As a method for deactivating the security function, for example, a method described in Japanese Application No. 2000-121844, supra, may be employed, in which read operations are performed to the addresses of the memory rewriting unit 214 in a certain sequence, and in which the security function is deactivated only when the values and order of the addresses match those stored in the address storing regions 1 to N in the memory rewriting unit 214.

[0109] The security deactivation as described above is performed by the security control circuit 217, which outputs a security control signal 218 for instructing deactivation of the security function to the operation restriction circuit 219. Once receiving the security control signal 218 which instructs the deactivation of the security function, the operation restriction circuit 219 no longer applies restriction on any erase operations which are requested to be performed. As a result, erase operations can take place properly.

[0110] As the security control circuit 217, a circuit which examines an order in which a number of addresses were accessed, e.g., as described in Japanese Application No. 2000-121844, supra, plus additional latch circuitry for latching the content which is stored in the address storing regions 1 to N and which is read via the data signal 212, may be employed. The latched address(es) may be used as reference addresses.

[0111] In the present example, all of the contents stored in the address storing regions 1 to N are erased when the data stored in the memory rewriting unit 214 is erased. However, the data stored in the memory rewriting unit 214 is not erased unless all of the address storing regions 1 to N contain addresses stored therein. Thus, there is provided an advantage in that redundant erase operations can be automatically prevented since the contents stored in the memory rewriting unit 214 and the contents stored in the address storing regions 1 to N within the memory rewriting unit 214 are simultaneously erased, thereby eliminating the need to perform any further erasure.

[0112] Thus, the present example solves a problem which is associated with a structure in which address storing regions are provided in a memory rewriting unit other than the memory rewriting unit 214 because, in such a structure, it would be necessary to perform two erase operations, i.e., one for erasing the data stored in the memory rewriting unit 214 and another for erasing the contents stored in the address storing regions; otherwise, a special technique for effecting simultaneous erase operations would be required.

[0113] Furthermore, in the present example, it is possible to additionally employ the data storage section (data storing regions) illustrated in Example 2 of the present invention. In that case, it may be ensured that each erase operation performed also results in the erasure of any corresponding data stored in the data storing region. This can be realized, without entailing any increase in the number of erase operations to be performed, by providing the data storing regions within the same memory rewriting unit.

[0114] According to the present example, the same type of semiconductor memory cells as those already employed in the semiconductor device can be utilized as an address storage section. Therefore, it is not necessary to additionally employ any circuitry or manufacture processes which would be required for other types of memory cells.

[0115] For example, in embodiments where erase operations for volatile semiconductor memory cells are to be restricted, any data stored in the semiconductor memory cells will be lost as the supply of power is terminated. In this case, it is preferable that the address storage section is also volatile because using non-volatile memory cells for the address storage section, which is designed for the purpose of restricting erase operations, would bring about nothing but the extra complexity of having to perform an overwrite operation after

the device is turned ON in order to clear the content which is already stored in the address storage section.

[0116] On the other hand, in the case where the semiconductor device incorporates non-volatile semiconductor memory cells, any data stored therein will not be lost after power termination. In this case, it is preferable to employ non-volatile means for the address storage section in order to continuously apply restriction on erase operations to protect the stored data after the device is turned ON again.

[0117] According to the present example, regardless of whether the semiconductor device incorporates volatile or non-volatile semiconductor memory cells, a satisfactory address storage section which has the same characteristics as those of the data storage means (i.e. a memory device) can be provided.

[0118] In the case where the present example is embodied with a flash EEPROM, in which any erasure will occur on a block-by-block basis, it is possible to prevent unauthorized overwriting to some degree by simply prohibiting erase operations. In the case where the address storage section is implemented as flash EEPROM cells within a block for which erasure is prohibited, the addresses which were stored in the address storage section will be erased during an erase operation after the security function is deactivated. Therefore, it is possible to arrange the device so that a predetermined overwriting procedure will be started anew after erasure, without having to separately clear the address storing regions.

[0119] By providing an address storage section for erasure restriction purposes for each block, there is provided an additional advantage in that each address to be stored in the address storage section only needs to be representative of a location within each block, so that a smaller number of bits need to be stored, if at all. This enhances the scale economy associated with the address storing regions and/or the comparison circuits.

(Example 4)

[0120] Figure 4 is a schematic block diagram illustrating a semiconductor device 350 according to Example 4 of the present invention. The semiconductor device 350 includes an interface circuit 304, a security circuit 309, and a memory 313 having a memory space composed essentially of rewritable semiconductor memory cells. The security circuit 309 includes: an address storage control circuit 314; an address storage circuit section 316 capable of storing N addresses (where N is a natural number); a reference address storage circuit section 322 capable of storing M predetermined addresses data (where M is a natural number); a security control circuit 319; and an operation restriction circuit 321 for restricting the operations to be performed on the memory 313. The security circuit 309 functions as a control circuit for the memory 313.

[0121] In the present example, it is assumed that the address storage circuit section 316 includes N address

storage circuits 1 to N, such that each of the address storage circuits 1 to N stores one address. It is also assumed that the reference address storage circuit section 322 includes M reference address storage circuits 1 to M, such that each of the reference address storage circuits 1 to M stores one reference address. Although the following description is directed to a case where $N=M$, the present example is not limited thereto.

[0122] All of the component elements of the semiconductor device 350 may be provided on one device to realize a security function for the memory 313. However, it is not necessary to provide all of the aforementioned component elements on a single device. For example, the security function may be realized on a number of devices collectively, e.g., by employing a separate security device, which includes the interface circuit 304 and the security circuit 309, to control the memory 313.

[0123] The reference address storage circuit section 322 stores predetermined reference addresses (1 to M). The reference address storage circuit section 322 may be arranged so as to be rewritable by providing a dedicated control circuit. Alternatively, any signals which are derivable from fixed circuitry may be employed as reference addresses.

[0124] In the present example, the memory 313, the interface circuit 304, the address storage circuit section 316, and the operation restriction circuit 321 may be implemented by using similar means to the memory 13, the interface circuit 4, the address storage circuit section 16 and the operation restriction circuit 20 of the semiconductor device 50 according to Example 1 of the present invention.

[0125] An address signal 301, a control signal 302, and a data signal 303 are externally input to the semiconductor device 350 to request overwriting of data stored at a given address of the memory 313. Upon recognizing the request, the interface circuit 304 outputs an internal control signal 306 to the address storage control circuit 314. The address storage control circuit 314 issues an address storage control signal 315 to store the address for which overwrite has been requested in any address storage circuits 1 to N in the address storage circuit section 316 where addresses are not stored yet. In doing so, it is ensured that addresses are sequentially stored in the address storage circuits 1 to N, beginning from the address storing circuit 1. If all of the address storage circuits 1 to N already contain addresses stored therein, the address storage control circuit 314 stores no more addresses in the address storage circuit section 316. As the addresses to be stored, only portions of each address may be stored, rather than all bits of the address, because the order of overwriting is significant, as opposed to the address value itself.

[0126] In one embodiment, the security control circuit 319 at least includes a comparison circuit for comparing, in the case where all of the address storage circuits 1 to N contain addresses stored therein, each address (address signal 317) stored in the address storage circuit

section 316 against each address (reference address signal 318) stored in the reference address storage circuit section 322. Only if all the addressee match does the security control circuit 319 output a security control signal 320 for deactivating the security function to the operation restriction circuit 321, whereby overwriting operations to the memory 313 will be permitted. If the address signal 317 and the reference address signal 318 do not match, the operation restriction circuit 321 applies restriction on some or all of the operations to be performed on the memory 313.

[0127] As a method for restricting some or all of the operations to be performed on the memory 313, any one of the following methods may be employed, without limitation: a method in which the address (as represented by the internal address signal 305) for which an operation is sought is modified so as to be output as an address signal 310 to the memory 313; a method which involves withholding the issuance of a control signal 311 to the memory 313; or a method which involves introducing some modification between the internal data signal 308 and the data signal 312.

[0128] Although the above description illustrates a case where the number (N) of address storage circuits in the address storage circuit section 316 and the number (M) of reference address storage circuits in the reference address storage circuit section 322 are equal (N=M), the present invention is not limited to such a structure. In the case where N is not equal to M, the security control circuit 319 may compare any information associated with the address(es) stored in the address storage circuit section 316 against any information associated with the reference address(es) stored in the reference address storage circuit section 322.

[0129] In the case where the overwriting of the memory 313 is not restricted in the initial state, any overwriting which is requested in an order not conforming to a predetermined order will result in the restriction of subsequent overwriting, whereby unauthorized overwriting can be prevented. In the case where the overwriting of the memory 313 is restricted in the initial state, the restriction on overwriting is deactivated in response to an overwriting which is requested in an order conforming to the predetermined order, thereby only preventing unauthorized overwriting.

[0130] In the present example, for example, a circuit which examines an order in which a number of addresses were accessed may be used as the security control circuit 319, e.g., as described in Japanese Application No. 2000-121844, *supra*.

[0131] In Examples 1 to 4, in the case where non-volatile memory cells are employed as address storage circuits, it is possible to realize an arrangement in which a single instance of requesting overwriting in the wrong order will result in perpetual prohibition of overwriting, whereby enhanced security can be provided.

[0132] On the other hand, in the case where volatile memory cells are employed as address storage circuits,

even if overwriting is requested in the wrong order, the address storage circuits can always be reset, e.g., by once turning the device OFF and then ON, whereby the history of any overwriting requested in the wrong order can be cleared. As a result, another opportunity for deactivating restriction on overwriting will be given.

[0133] Note that the security function according to the present invention can be controlled on the basis of any information associated with the address(es) which is output from the address storage circuit section and/or the data which is output from the data storage circuit section, rather than such addresses and/or data themselves.

[0134] A third party who wishes to attempt any unauthorized use of a semiconductor device to which the present invention is applied will have to know the exact principle of unauthorized overwriting prevention according to the present invention as well as any and all previously stored addresses, in order to completely fully overwrite the stored contents. Thus, any unauthorized access by a third party not having such information can be very effectively blocked.

[0135] The present invention is generally applicable to any semiconductor device that incorporates a circuit which functions as a memory, as well as commonly-used memory devices. For example, the present invention finds use in processors having internal memories, LCD controllers having internal VRAMs, and the like.

[0136] As described above, according to the present invention, a formidable security function for a semiconductor device having rewritable semiconductor memory cells can be provided without requiring any special devices external to the semiconductor device, such that it is difficult for any third party to decipher the method for controlling the security function. Thus, unauthorized access can be very effectively blocked while minimizing the influences on product size and/or cost.

[0137] Various other modifications will be apparent to and can be readily made by those skilled in the art without departing from the scope and spirit of this invention. Accordingly, it is not intended that the scope of the claims appended hereto be limited to the description as set forth herein, but rather that the claims be broadly construed.

Claims

1. A semiconductor device comprising:

- a memory having a memory space for recording data, the memory space including addresses;
- at least one first storage section for storing at least a portion of an address at which access to the memory space is requested and/or data which is requested to be written to the memory space; and

- an operation restriction circuit for at least partially restricting operations to be performed on the memory,
wherein the operation restriction circuit controls restriction on the operations to be performed on the memory based on at least a portion of the data and/or the address stored in the at least one first storage section. 5
2. A semiconductor device according to claim 1, wherein the access is a write operation. 10
3. A semiconductor device according to claim 1, wherein the at least one first storage section comprises a plurality of storage subsections. 15
4. A semiconductor device according to claim 1, wherein, if at least one of the at least one first storage section does not contain the address or data stored therein, the operation restriction circuit maintains restriction on the operations to be performed on the memory. 20
5. A semiconductor device according to claim 1, wherein: 25
- the at least one first storage section includes an address storage section for storing the address, and a data storage section for storing the data: 30
- the semiconductor device includes a comparison circuit for performing a comparison of data in the memory space as designated by the address stored in the address storage section against the data stored in the data storage section; and 35
- the operation restriction circuit maintains restriction on the operations to be performed on the memory if a result of the comparison by the comparison circuit does not match. 40
6. A semiconductor device according to claim 1, further comprising: 45
- a second storage section for storing a reference address; and 50
- a comparison circuit for performing a comparison of the address stored in the first storage section against the reference address stored in the second storage section, 55
- wherein the operation restriction circuit deactivates restriction on the operations to be performed on the memory if a result of the comparison by the comparison circuit matches.
7. A semiconductor device according to claim 1, wherein:
- the memory includes a storage unit for containing data which is to be concurrently rewritten; and
the first storage section is included in the storage unit.
8. A control device for controlling a memory having a memory space for recording data, the memory space including addresses, the control device comprising: 60
- at least one first storage section for storing at least a portion of an address at which access to the memory space is requested and/or data which is requested to be written to the memory space; and
an operation restriction circuit for at least partially restricting operations to be performed on the memory, 65
- wherein the operation restriction circuit controls restriction on the operations to be performed on the memory based on at least a portion of the data and/or the address stored in the at least one first storage section.
9. A control device according to claim 8, wherein the access is a write operation. 70
10. A control device according to claim 8, wherein the at least one first storage section comprises a plurality of storage subsections. 75
11. A control device according to claim 8, wherein, if at least one of the at least one first storage section does not contain the address or data stored therein, the operation restriction circuit maintains restriction on the operations to be performed on the memory. 80
12. A control device according to claim 8, wherein: 85
- the at least one first storage section includes an address storage section for storing the address, and a data storage section for storing the data; 90
- the semiconductor device includes a comparison circuit for performing a comparison of data in the memory space as designated by the address stored in the address storage section against the data stored in the data storage section; and 95
- the operation restriction circuit maintains restriction on the operations to be performed on the memory if a result of the comparison by the comparison circuit does not match.
13. A control device according to claim 8, further comprising: 100

a second storage section for storing a reference address; and
a comparison circuit for performing a comparison of the address stored in the first storage section against the reference address stored in the second storage section,
wherein the operation restriction circuit deactivates restriction on the operations to be performed on the memory if a result of the comparison by the comparison circuit matches.

14. A control device according to claim 8, wherein:

the memory includes a storage unit for containing data which is to be concurrently rewritten;
and
the first storage section is included in the storage unit.

20

25

30

35

40

45

50

55

FIG. 1

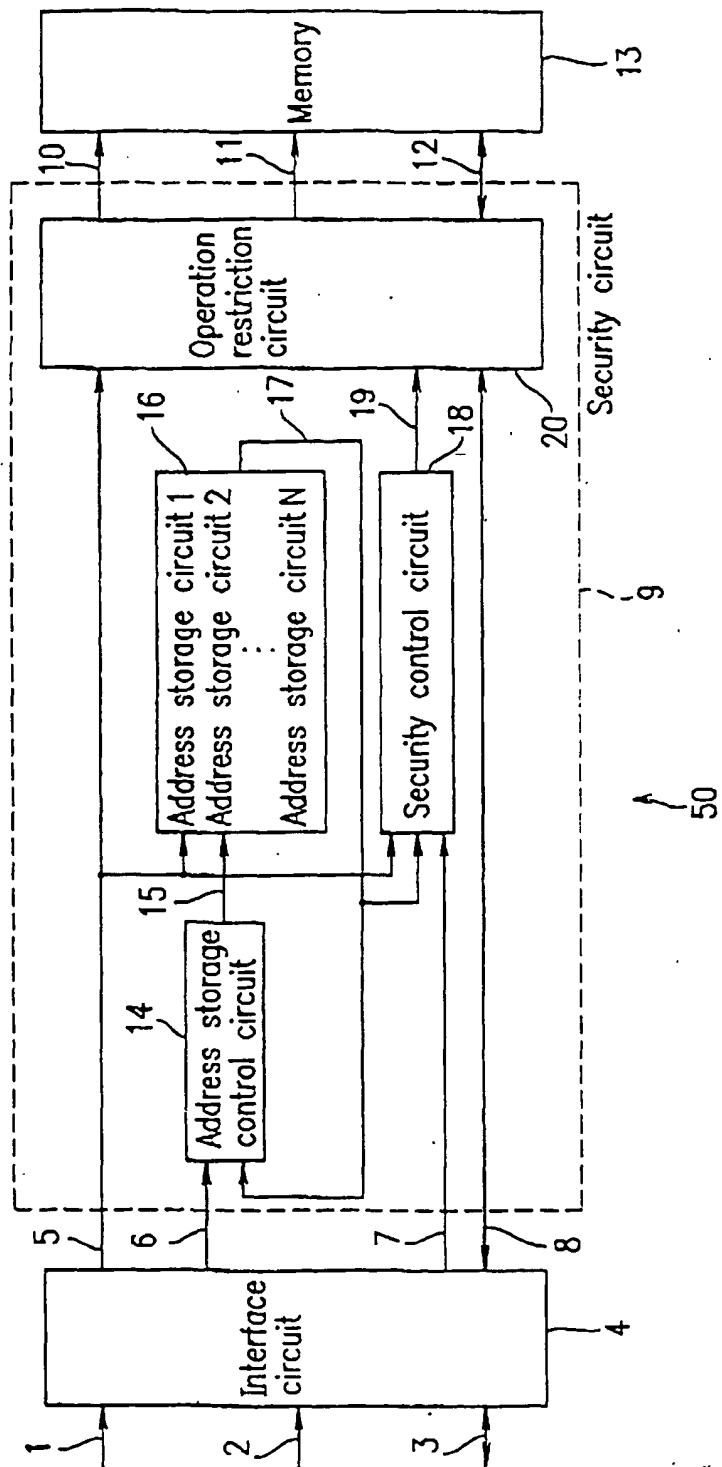


FIG. 2

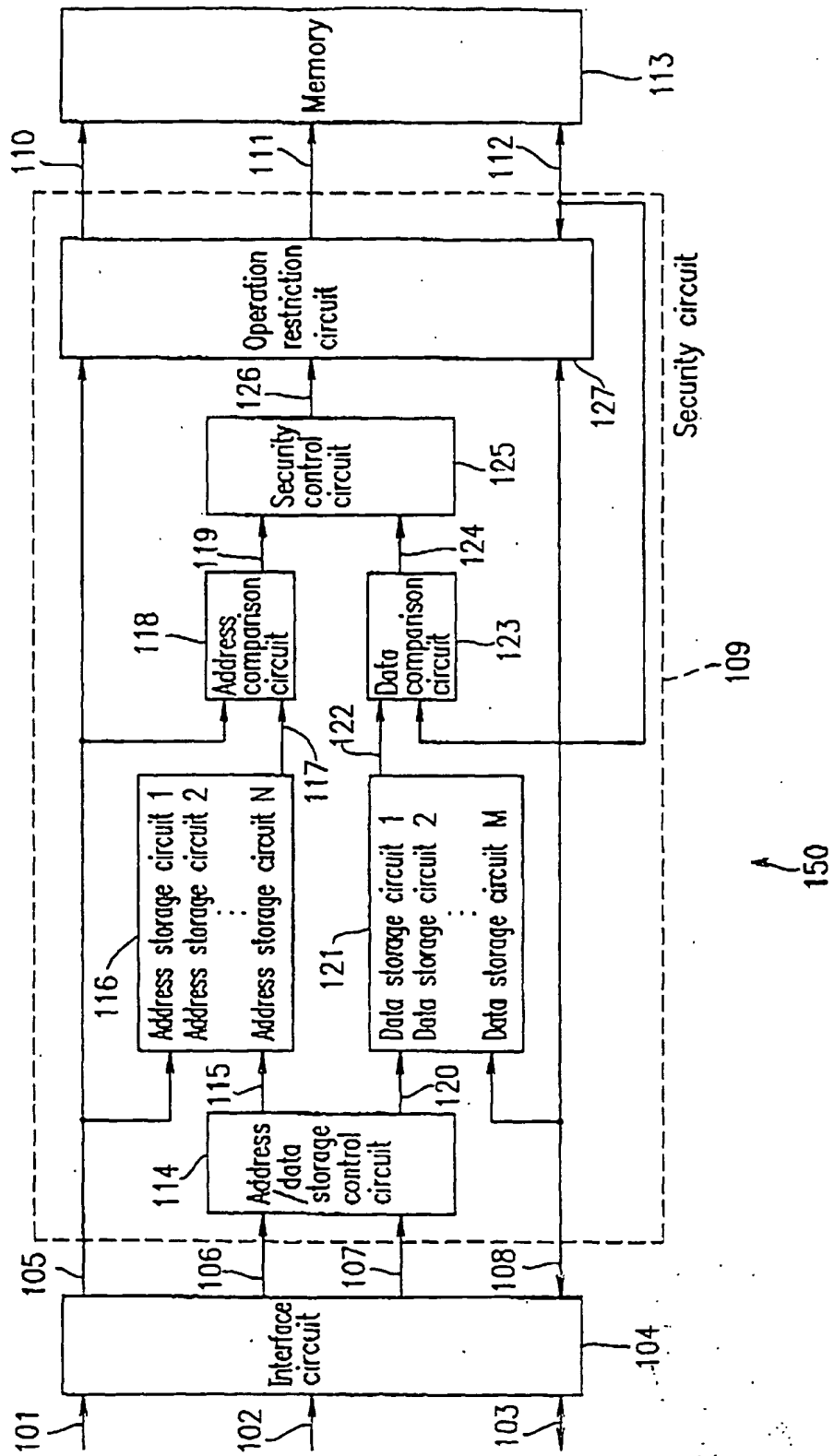


FIG. 3

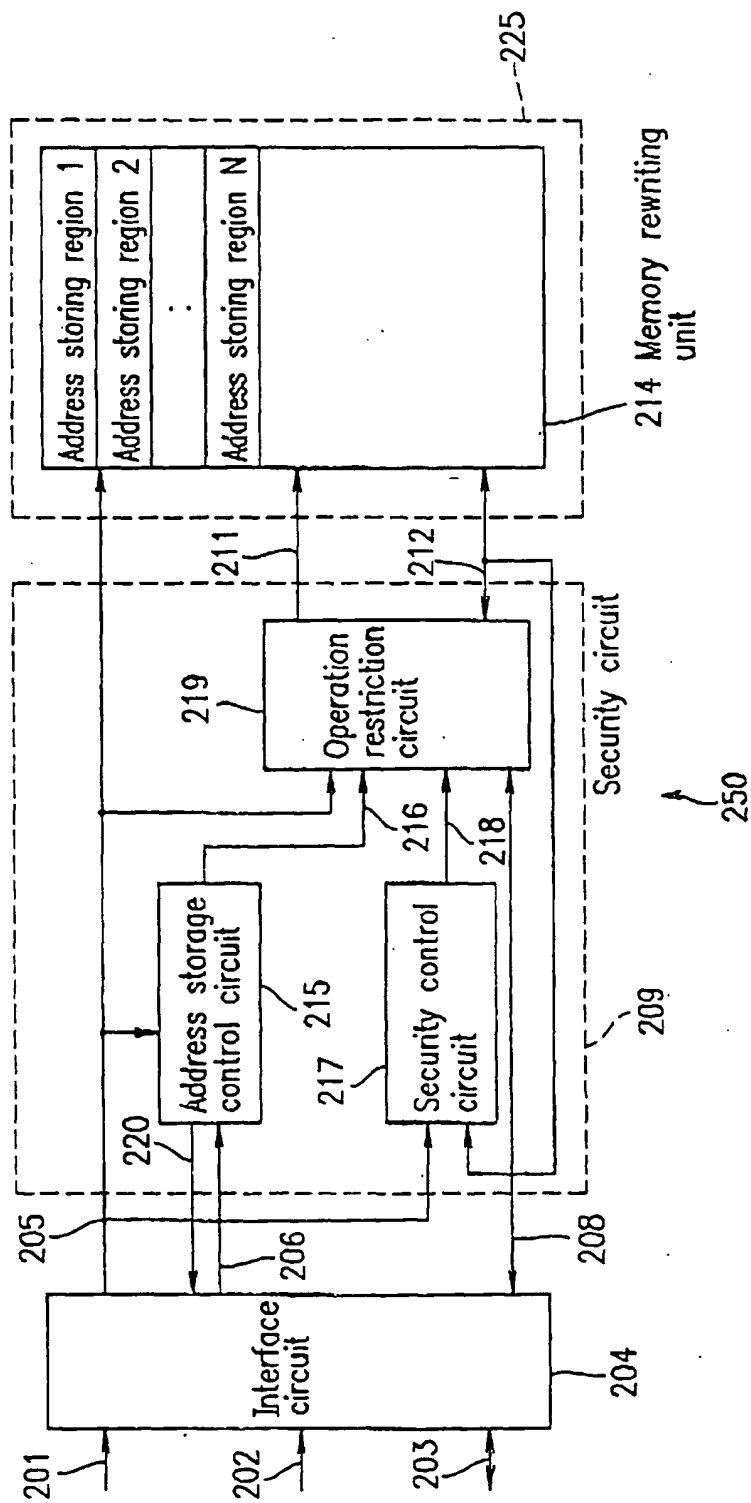


FIG. 4

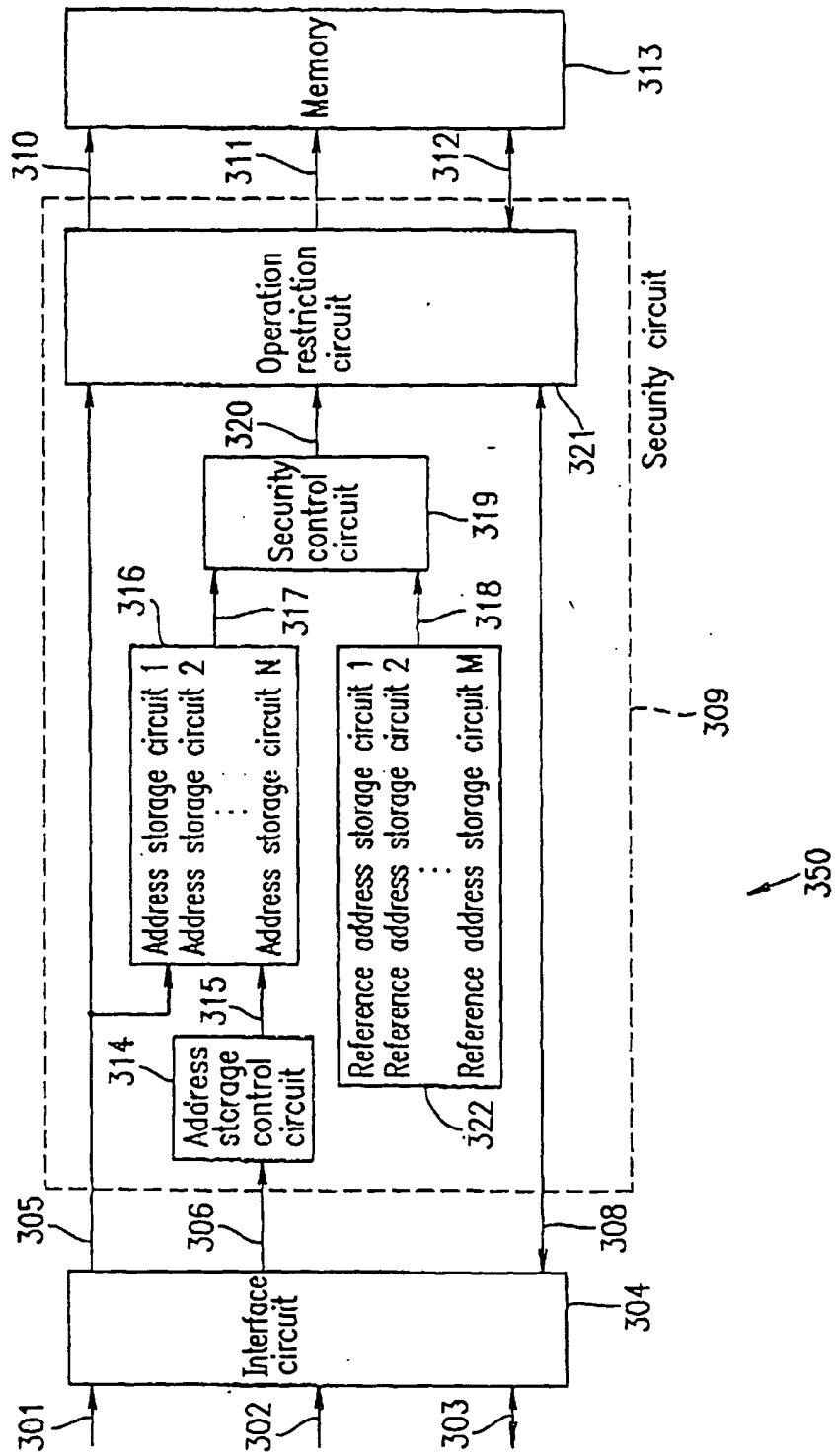


FIG. 5

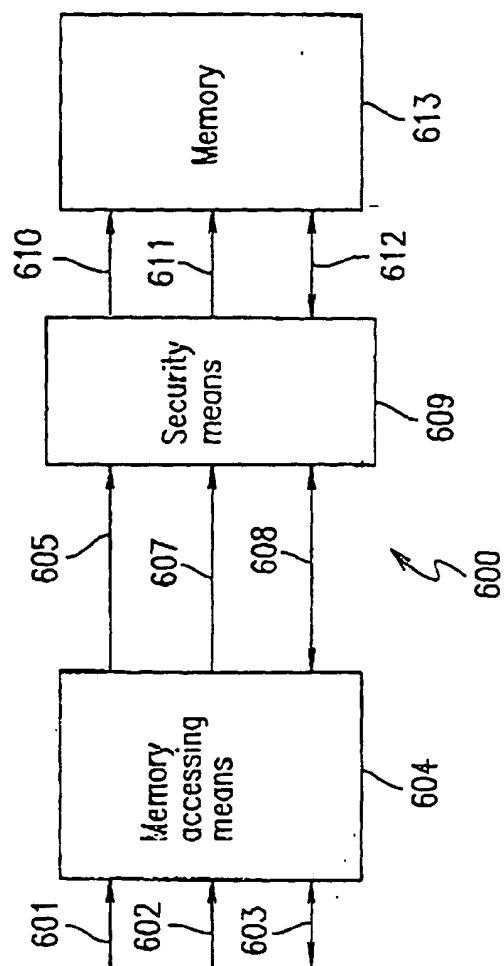


FIG. 6

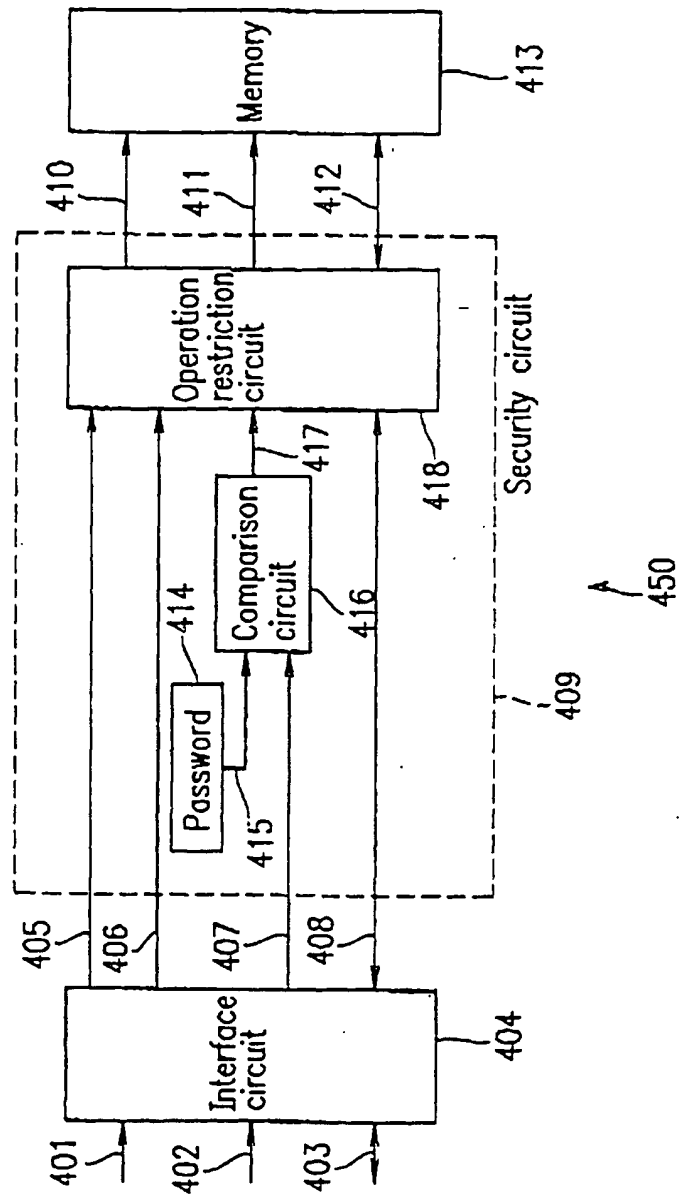
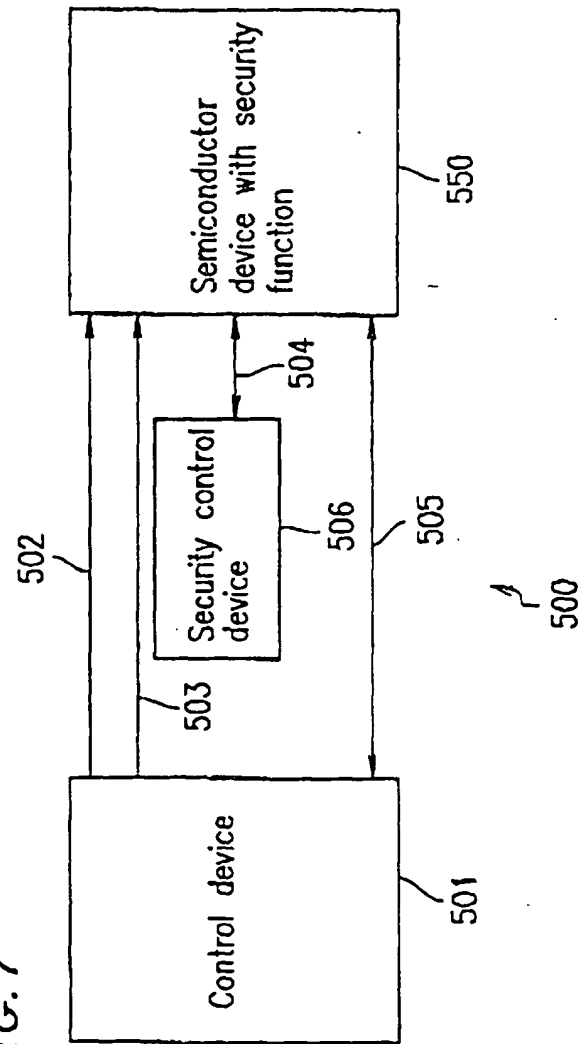


FIG. 7





European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 30 5122

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	PATENT ABSTRACTS OF JAPAN vol. 1999, no. 13, 30 November 1999 (1999-11-30) & JP 11 213680 A (FUJITSU LTD), 6 August 1999 (1999-08-06) * abstract *	1-4,8-11	G11C16/22 G11C8/00 G11C7/24
Y	* abstract *	5,12	
P,X	& US 6 215 717 A (TAKEGUCHI) 10 April 2001 (2001-04-10) * column 5, line 21 - column 8, line 17; claims 1,2; figures 6,7,12 *	1-4,8-11	
X	US 5 912 849 A (SAKAI HIROYUKI ET AL) 15 June 1999 (1999-06-15) * column 3, line 21 - line 65; figures 16-18 *	1,6,8,13	
Y	US 6 061 280 A (ARITOME SEIICHI) 9 May 2000 (2000-05-09) * abstract * * column 16, line 29 - line 34; figure 21 * -----	5,12	
			TECHNICAL FIELDS SEARCHED (Int.Cl.7)
			G11C
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 9 October 2001	Examiner Wolff, N
CATEGORY OF CITED DOCUMENTS X: particularly relevant if taken alone Y: particularly relevant if combined with another document of the same category A: technological background O: non-written disclosure P: intermediate document		T: theory or principle underlying the invention E: earlier patent document, but published on, or after the filing date D: document cited in the application L: document cited for other reasons &: member of the same patent family, corresponding document	

EPO FORM 1503 03/82 (P04C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 01 30 5122

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

09-10-2001

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
JP 11213680	A	06-08-1999	US	6215717 B1	10-04-2001
US 5912849	A	15-06-1999	US	5818771 A	06-10-1998
			JP	10106275 A	24-04-1998
US 6061280	A	09-05-2000	JP	10199265 A	31-07-1998

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82